BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C.

In the matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information;	)	
	)	RM-11277
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	

COMMENTS OF RNK INC. D/B/A RNK TELECOM

In response to the Federal Communications Commission's (the "Commission") Notice of Proposed Rulemaking issued in the above-captioned proceedings and the Electronic Privacy Information Center's ("EPIC") Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information,[1] RNK Inc. d/b/a RNK Telecom ("RNK"), by its attorneys, hereby respectfully submits the following comments.

I. INTRODUCTION

RNK Inc., a small, privately-held company, based in Dedham, Massachusetts, and founded in 1992, has grown from its initial niche of local resale and prepaid long distance calling cards to an Integrated Communications Provider, marketing local and interexchange telecommunications services, as well as Internet Services

[1] *See CPNI,* Notice of Proposed Rulemaking ("CPNI NPRM"), CC Docket No. 96-115 *(released Feb. 14, 2006)* and *Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005).*

and IP-enabled services. RNK is a registered Competitive Local Exchange Carrier ("CLEC") in Massachusetts, Rhode Island, New York, New Jersey, New Hampshire, Connecticut, and Florida, and offers wholesale and retail residential and business telecommunications services via resale and its own facilities. In addition, RNK has interexchange ("IXC") authority in Vermont, Florida, and Maine, as well as international 214 authority from the Federal Communications Commission ("FCC" or "Commission"). Via its own facilities, RNK serves a variety of customers, including IP-Enabled telephone customers, with a broad range of telecommunications and non-telecommunications services.

II. THE INDIRECT RELATIONSHIP OF WHOLESALE CARRIERS WITH END-USERS SHOULD BE CONSIDERED IN THE ESTABLISHMENT OF ANY STANDARDS OR RULES FOR THE PROTECTION OF CPNI.

RNK shares the Commission's well-founded concern regarding the protection of private customer proprietary information collected and held by telecommunications carriers.[2] As further explained below, RNK believes that flexible standards and rules that take into account a variety of relationships, such as that of wholesale carriers that have end-users (i.e., whether there is a direct or indirect relationship), are most prudent and would best accomplish the Commission's goal of protecting CPNI without unduly burdening carriers, with little to no benefit for consumers.

A. Consumer-Set Passwords versus Biological Information to Identify Customers.

In its petition, EPIC expressed great concern over the use of biological information (i.e., date of birth, mother's maiden name) to confirm the identity of individual's seeking customer information from a carrier's customer service department.

[2] *See* CPNI NPRM, at ¶ 1.

As an alternative, EPIC proposed that the Commission adopt a rule mandating that consumer's set their own passwords to increase the security of CPNI.[3] For RNK's IP-enabled service[4] customers, RNK has already implemented such a system successfully. These customers create their own username and password at the time of sign-up. Subsequently, these customers can view their secure CPNI by logging in to their individual "My Account" page, using the unique username they have chosen in addition to their current chosen password. They also have the ability to change their password at any time by contacting RNK's Network Operations Center ("NOC"), where a representative will verify certain key account information before allowing a password change to occur.[5] Essentially the same process is followed in the event a customer loses their password.

RNK is also a provider of telecommunications and wholesale "branded" IP-enabled services, which it sells to numerous resellers, who, in turn, resell those services to end-user consumers. The resellers' end-users are not aware that RNK is, in fact, their underlying service provider because all sign-up, billing and customer service is handled by the reseller. For these end-users, it is the reseller, and not RNK, that determines the management of their passwords. Some resellers provide their customers with pre-set passwords, while others will allow their end-users to set their own passwords. Because these resellers are wholly independent entities, RNK does not control or dictate the handling of these matters by each reseller. Indeed, as the wholesaler, RNK's role

---

[3] *See id.* at ¶ 15.

[4] In this context, the term "RNK's IP-Enabled services" refers to both RNK's direct retail services to customers and those sold at wholesale to other service providers and their end users on a private label basis.

[5] Currently, RNK does not permit passwords to be changed over the Internet and does not email passwords to end-users. In the near future, however, RNK will be able to send its customers information via a secure and encrypted on-line messaging system enabling it to forward passwords, and other CPNI, electronically to those customers able to verify certain account information.

regarding end-user passwords is quite limited. When IP-Enabled services customers or end-users require password changes, the corresponding equipment used by those customers or end users must be reconfigured to recognize this new password. For resellers, depending on a reseller's level of technical expertise, they may be able to perform these modifications themselves or may require RNK's assistance. Either way, RNK ultimately must process the password change in its system for the end-user's service to properly function with the new password. In these situations, when RNK is a wholesaler and the reseller is serving its customers, RNK does not interact with the end-user and therefore is not in a position to corroborate or question the legitimacy of any password change requests.

For its other, more "traditional," telecommunications and other services, RNK uses other methods to maintain the security of CPNI, alleviating the need to use biological information as an identifier of the individual seeking access to an account. By way of example, RNK's pre-paid calling card customers typically receive either a pre-assigned or randomly generated Personal Identification Number ("PIN") associated with their card. This PIN allows access to their accounts and/or calling information, and ideally, limits account access to only the person possessing the calling card — presumably the customer. However, because PINs can be lost, stolen or otherwise improperly obtained, RNK takes its identification process further, beyond the mere provision of the PIN by the individual calling to inquire about an account. Rather, RNK requires that the calling individual supply additional account information likely known

only by the actual end user.[6] This corroboration of information is a simple, efficient, and extremely useful tool that aids in maintaining the security of CPNI. It allows the carrier to avoid relying solely on PINs, which can easily be lost or stolen, or biographical information, which may have fallen into the hands of and/or are discoverable by unauthorized third persons, to identify and confirm that an authorized individual is in fact seeking the requested account information.

Consumer-set passwords provide greater protection and security for CPNI and the benefits of such a system far outweigh any burdens of implementation. RNK's end-users, like most consumers, are accustomed to using passwords to access their various accounts, and are in no way inconvenienced with these methods of securing access to their accounts. The role of the wholesaler, however, must be considered in the implementation of any rules intended to better protect CPNI, as the wholesaler often has little or no direct contact with end-user consumers, making it difficult for them to abide by rules that are overly broad and fail to address the dynamic created by the wholesaler/reseller/end-user relationship.

One means of accommodating wholesalers would be for the Commission to require even resellers of telecommunications or IP-enabled services to be responsible for protecting CPNI, and perhaps require these resellers to either comply, or obtain a written document from the underlying wholesaler, if that wholesaler has control over the end-users' CPNI, attesting to the fact that the wholesaler has adequately protected such CPNI.

B. Encryption of Customer Data Stored by Carriers

[6] In an abundance of caution, and per the Commission's suggestion, RNK is being intentionally vague as to the verifying information requested.

As part of its standard business arrangement with its IP-enabled service resellers, RNK provides each reseller with a branded end-user web page that the reseller can use to process orders for new customers and stay apprised of customer call and account activity. These branded web pages each have their own "hostname" IP addresses, which allow them to appear as separate individual websites. As such, these sites are directed to the wholesaler's "common name" IP address, which offers 128 bit in-transit encryption of customer application data via hypertext transfer protocol secure ("https"). Therefore, when RNK transfers sensitive customer data, including invoices, call detail records and credit card information, to and from its reseller account pages to its own back-end server, this information is highly encrypted while in-transit, and thus protected.

RNK understands the inherent dangers of exposing personalized customer data at its most vulnerable stage, that is, in transit over the public Internet. However, if a wholesaler like RNK, or, indeed, any service provider, were forced to expend a large amount of resources encrypting *stored* data maintained within its own private systems, as long as the systems are otherwise secure, the benefits of such encryption are less apparent. In the case of a hacker or other unauthorized person trying to "sniff" packets[7] while in transit, strong encryption, such as 256 bit, is an inexpensive and effective means of preventing theft of such data. In sharp contrast, encryption of stored data presents additional difficulties for both providers *and* consumers.

[7] "Sniff" refers to a program and/or device that monitor data traveling over a network. This monitoring can be used both for legitimate network management functions and for stealing information off a network. Unauthorized "sniffers" can be extremely dangerous to a network's security because they are hard to detect and can be inserted almost anywhere and, as such, they are a favorite weapon in the hacker's arsenal.

First and foremost, none of the manufacturers of the actual switches that create call detail records currently offer encryption of that stored data as an option. Because encryption of these stored records is not technically feasible, any rule mandating such a requirement would not only fail to improve the protection of CPNI, but would place numerous carriers in violation of a rule with which they have no conceivable means of complying.[8] If the Commission believes that the encryption of stored data is important and would have a meaningful impact on the protection of CPNI, then it could assume a leadership role in bringing equipment and software vendors together with service providers to develop and create new equipment and/or products able to provide encryption or other means of protection of the stored data at issue, and at affordable prices. In conjunction with this development process, the Commission might also consider, as it has done in the past, phasing in certain technical standards with which carriers would be required to comply over a period of time.

Secondly, even if the unavailability of equipment did not present the obstacles and limitations set forth above, issues of efficiency in providing and using encrypted stored CPNI still remain. For service providers, the encryption of stored data makes it significantly more difficult to offer services to end-users because encryption requires adding an extra de-encryption layer to every end-user service that makes use of the encrypted stored data. For RNK, which provides real-time views of nearly all account information to its end-users and resellers, the implementation of an encryption layer would make this voluminous data much more difficult to work

[8] Indeed, when Congress passed the Communications Assistance with Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279, it specifically provided for reimbursement for carriers and manufactures to bring equipment into compliance. The Commission should not use this proceeding to require such expensive alterations where even Congress did not.

with and the compilation of it into various reports, including those on demographics, port usage, fraud detection, subpoena requests, capacity monitoring, intercarrier compensation and billing, would be exceedingly difficult. Consequently, the encryption of this data would either restrict RNK's ability to provide its resellers and end-users with the information they seek and/or in the case of certain automated tools, offered by RNK to improve and simplify customer account access, the encryption layer would be rendered useless.

The minimal security gained by the encryption of stored CPNI is far outweighed by the inconvenience and lack of functionality in accessing account information that would result for service providers, resellers and end-users if such data were encrypted. Not only would the inclusion of a de-encryption layer make it more difficult for service providers to compile numerous reports and data for themselves and their customers, but it would ultimately result in a loss of account services and functionality – and such services and functionality are relied on by end-users and resellers to allow them to manage their businesses, services, and customers. More importantly, encrypted stored data is only as secure as the corporate computer network on which it resides. If hackers are able to gain access to a carrier's computer network, then in all likelihood they will gain access to CPNI, whether the stored data is encrypted or not, as there are other means of accessing this data without possessing the actual decryption key.[9]

[9] Also, when a reseller or end-user access CPNI on a website and then save the data to their own computer, the fact that the actual data stored by the service provider is encrypted is no guarantee of protection since that same information is now available on that individual's computer system, which likely has a lower level of security than the service provider's network.

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the rules[10] promulgated in support thereof offer some useful guidance on the issues presented in this proceeding. HIPAA was created to offer "strong protections for the privacy of individually identifiable health information."[11] Without doubt, an individual's medical information is some of the most private data in existence and is at least as sensitive, if not more so, than the CPNI at issue here. Notably, however, the HIPAA rules do not mandate encryption of stored data.[12] Rather, these rules provide for security standards that are technology neutral, allowing organizations to make their own technology choices, and with regard to encryption of stored data, based upon the entity's risk analysis. These rules recognize that by avoiding requirements of specific technologies, which will likely become obsolete, the industry will be better able to apply innovation to protect sensitive data.[13]

The same reasoning is applicable to the instant issue. Because changes in technology occur rapidly, it is important that the Commission establish CPNI security standards general enough to withstand these changes over time. In the long run, more general encryption standards will better protect CPNI by allowing service providers to enhance security proactively over time with technologies that today are impractical or do not even exist. Without this sort of flexibility, it will be exceedingly difficult for carriers to stay one step ahead of data thieves.

C. Notice

---

[10] 45 C.F.R. pts. 160, 162 and 164.
[11] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53182 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160 and 164).
[12] *See* 45 C.F.R. § 164.312.
[13] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (Feb. 20, 2002) (codified at 45 C.F.R. pts. 160, 162 and 164).

The Commission has requested comment on whether, as a safeguard measure, carriers should be required to notify customers whenever their CPNI is released.[14] This proposition evolved from EPIC's statement that such "notification could help the affected individual mitigate any harm from [a] security breach."[15] A rule mandating such notification, however, would be overly broad, as it would include situations where the carrier has no grounds to suspect that the request for CPNI was not legitimate, such as when a reseller queries a wholesaler for billing information which it needs to carryout its business.[16] Moreover, for several reasons, the underlying wholesalers of telecommunication and IP-enabled services are not in the position to notify resellers' or retail customers' end-users when their CPNI is released or accessed.

RNK provides it resellers with a branded end-user webpage, which is used by the reseller not only to obtain new customers, but to check and review various call detail records and other proprietary data pertaining to its customers and/or end users. Not surprisingly, most resellers, via these webpages, regularly access and review various CPNI in the regular course of their daily business. If notice to customers was required every time their CPNI was accessed or released, then on each occasion that a reseller reviewed its customer's records, possibly several times each day depending on the number of customers a reseller might have, the wholesaler would be obliged to somehow notify the end-user, with whom it has no direct relationship, of such activity.

[14] *See* CPNI NPRM at ¶¶ 21-23.
[15] *Id.* at ¶ 21.
[16] *See id.* at ¶ 23.

Such a rule would not only result in the wholesaler expending excessive amounts of time and resources providing notice of harmless activity, but would also be a nuisance to most customers, who likely have little desire to know when their telephone or IP-enabled services company, with whom they have entered into a business relationship, is reviewing such information as a regular part of the resellers business tasks. This responsibility would instead fall to the reseller, and is another reason to include resellers in the CPNI security/verification process, as stated above.

Therefore, much like the Commission's Universal Service Fund payment, pay phone compensation, and other "shared" responsibility schemes,[17] in addition to requiring resellers to be responsible for CPNI compliance, RNK believes that the Commission should make an explicit "carve-out" or exemption for wholesale carriers and their release of CPNI to reseller "customers," based on the releasing carrier's good faith belief that the recipient of such information is using the information for its provision of telecommunications and/or IP-enabled equivalents thereof. The "carve-out" should cover transactions with the following types of recipients: (1) a reseller, re-brander, or similar entity where the receiving entity has the responsibility for direct end-user contact; (2) a local exchange carrier and/or interexchange carrier or similar IP-enabled provider that receives, what in its judgment is a *bona fide* order or request for services, in an industry-standard form (when applicable), including, but not limited to, an Access Service Request ("ASR"), Local Service Request ("LSR"), or Customer

[17] In each of these FCC regulatory schemes, the last "carrier" in line or provider of services to the end-user/customer is responsible for action/payment, and the "down stream" carriers/providers are responsible for reporting, but are exempted from action/payment.

Account Record Exchange ("CARE") transmission. Further, RNK believes that customers should be informed when they initially sign-up with their service provider that CPNI will be divulged to appropriate parties solely for the purpose of providing services ordered by the customer. In exchange, these entities, and those mentioned above would be required to agree, subject to Commission sanction and/or private right of action, that they will only use CPNI for such intended uses and will limit the disclosure to only that information necessary to complete the task at hand.

Such reasonable limits on notification will not only ease the logistical and what could be severe financial burdens on service providers merely trying to provide services to their reseller customers, and end users, but will also lessen the possibility of consumer confusion resulting from frequent and/or multiple notices that are required to provide and maintain their services.

III. CONCLUSION

For all of the reasons stated herein, RNK urges the Commission to consider the indirect relationship of wholesale service providers to end-users in promulgating any rules to further protect CPNI. In doing so, the Commission should either include resellers in the FCC's requirements for CPNI security and a simultaneous carve out exception for wholesale carriers, who have little to no contact with end-users or, in the alternative, should establish flexible rules specific to wholesale carriers.

The more stringent standards proposed by EPIC are flawed in that they cast too wide a net and operate on the erroneous assumption that all holders of CPNI have direct contact with end-users. Instead, outcome-based standards, as opposed

to those that specify technical solutions, will prove more beneficial to both carriers and end-users long-term. RNK looks forward to working with the Commission to further develop these ideas.

Respectfully submitted, by its Attorney

/s/

Douglas Denny-Brown
Sharon R. Schawbel
Matthew T. Kinney
RNK Inc. d/b/a RNK Telecom
333 Elm Street, Suite 310
Dedham, MA 02026
(781) 613-6000

Dated: April 28, 2005